

This listing of claims will replace all prior versions, and Listings of Claims in the application:

Listing of Claims:

Claim 1 (Currently amended): A method for accessing a session comprising:
converting a first token of one or more tokens assigned to a user to an authenticated token, said authenticated token incorporating a user identity and having a different content from said first token;

associating said user with said session using said authenticated token; and

presenting said authenticated token to access said session from a first terminal;

authenticating said user implementing a second token, the authenticating using the second token being converted to a same authentication for said user as the authenticated token created from the first token,

wherein each token of the one or more tokens assigned to said user can be implemented to authenticate said user, and further wherein the one or more tokens assigned to said user can be converted to said authenticated token, said authenticated token capable of providing access to said session from a second terminal while said session is being accessed from said first terminal.

Claim 2 (Canceled)

Claim 3 (Previously presented): The method of claim 1 further comprising:
sending a session disconnect signal to said first terminal; and
routing input and output for said session to said second terminal.

Claims 4-7 (Cancelled)

Claim 8 (Previously Presented): The method of claim 43 wherein said biometric identifier is a finger print pattern.

Claim 9 (Previously Presented): The method of claim 8 wherein said biometric identifier is a retinal image.

Claim 10 (Cancelled)

Claim 11 (Previously Presented): The method of claim 1 wherein said session is identified by said authenticated token.

Claim 12 (Currently amended): A session accessing system comprising:
an associating unit configured to associate a user with a session using an authenticated token created using an initial token of one or more tokens assigned to said user, said associating unit including,

a first converting unit configured to convert said initial token to said authenticated token, said authenticated token incorporating a user identity and having a different content from said first token; [[and]]

a first presenting unit configured to present said authenticated token to access said session from a first terminal; and

a second converting unit configured to convert a second token to said authenticated token, the second token being converted to a same authentication for the user as the authenticated token created from the initial token,

wherein each token of the one or more tokens assigned to said user can be presented to a second presenting unit to authenticate said user, and further wherein the one

or more tokens assigned to said user can be converted to said authenticated token, said authenticated token capable of providing access to said session from a second terminal while said session is still being accessed from said first terminal.

Claim 13 (Canceled)

Claim 14 (Previously presented): The session accessing system of claim 12 further comprising:

a messaging unit configured to send a session disconnect signal to said first terminal; and

a routing unit configured to route input and output for said session to said second terminal.

Claim 15 (Previously presented): The session accessing system of claim 12 wherein said associating unit further comprises:

an authentication unit configured to authenticate an identity of said user implementing said initial token.

Claim 16 (Previously Presented): The session system of claim 15 wherein said authentication unit comprises:

a user interface configured to obtain said initial token, said initial token being a physical token assigned to said user, a passphrase, or a biometric identifier.

Claim 17-18 (Cancelled)

Claim 19 (Previously Presented): The session accessing system of claim 16 wherein said biometric identifier is a finger print pattern or a retinal image.

Claims 20-22 (Cancelled)

Claim 23 (Currently amended): A computer program project comprising:
a computer usable medium having computer readable program code embodied therein configured for accessing a session, comprising:

computer readable code configured to convert a first token of one or more tokens assigned to a user to an authenticated token, said authenticated token incorporating a user identity and having a different content from said first token;

computer readable code configured to cause a computer to associate said user with said session using said authenticated token; [[and]]

computer readable code configured to cause a computer to present said authenticated token to access said session from a first terminal; and

computer readable code configured to authenticate said user implementing a second token, the second token being converted to a same authentication for said user as the authenticated token created from the first token,

wherein each token of the one or more tokens assigned to said user can be implemented to authenticate said user, and further wherein each token of the one or more tokens assigned to said user can be converted to said authenticated token, said authenticated token capable of providing access to said session from a second terminal while said session is still being accessed from said first terminal.

Claim 24 (Canceled)

Claim 25 (Previously presented): The computer program product of claim 23 further comprising:

computer readable code configured to cause said one or more computers to send a session disconnect signal to said first terminal; and

computer readable code configured to cause-said one or more computers to route input and output for said session to said second terminal.

Claims 26-33 (Cancelled)

Claim 34 (Canceled)

Claim 35 (Currently amended) A method for accessing a session comprising:
authenticating an identity of a user implementing a first token of one or more tokens assigned to said user;

converting said first token of one or more tokens to an authenticated token, said authenticated token incorporating a user identity and having a different content from said first token;

associating said user with said session using said authenticated token;

presenting said authenticated token to access said session from a first terminal,

wherein said authenticated token may be created using each token of the one or more tokens; the method further comprising,

authenticating said identity of said user implementing a second token of one or more tokens assigned to said user, the authenticating using the second token being converted to a same authentication for said user as the authenticated token created from the first token;

~~converting said second token of one or more tokens to said authenticated token;~~

and

presenting said authenticated token to access said session from a second terminal while said session is still being accessed from said first terminal.

Claim 36 (Previously Presented): The method of claim 35 further comprising:
sending a session disconnect signal to said first terminal; and
routing input and output for said session to said second terminal.

Claim 37 (Previously Presented): The method of claim 35 wherein said first token and said second token are the same token.

Claim 38 (Previously Presented): The method of claim 35 wherein said first token and said second token are different tokens.

Claim 39 (Previously Presented): The method of claim 35 wherein said step of authenticating said identity of said user using said first token includes obtaining said first token of said one or more tokens, and further wherein said step of authenticating said identity of said user using said second token includes obtaining said second token.

Claim 40 (Previously Presented): The method of claim 39 wherein each token of one or more tokens can be one of a biometric identifier, a physical token, and a passphrase.

Claim 41 (Previously Presented): The method of claim 40 wherein said biometric identifier is one of a finger print pattern and a retinal image.

Claim 42 (Previously presented): The method of claim 1 wherein said first token is the same as said second token or said first token is different from said second token.

Claim 43 (Previously Presented): The method of claim 42 wherein said step of associating comprises:

obtaining said first token, said first token being a physical token assigned to said user, a passphrase, or a biometric identification.

Claim 44 (Previously Presented): The method of claim 42 further comprising:

obtaining said second token, said second token being a passphrase, a physical token assigned to said user, or a biometric identifier.

Claim 45 (Previously Presented): The method of claim 44 wherein said biometric identifier is a fingerprint pattern.

Claim 46 (Previously Presented): The method of claim 45 wherein said biometric identifier is a retinal image.

Claim 47 (Previously presented): The computer program product of claim 23 wherein said first token is the same as said second token or said first token is different from said second token.

Claim 48 (Previously Presented): The computer program product of claim 47 further comprising:

computer readable code configured to cause said one or more computers to authenticate an identity of said user implementing each token of the one or more tokens, said computer readable code including,

computer readable code configured to cause said one or more computers to obtain said first token of said one or more tokens, and computer readable code configured to cause said one or more computers to obtain said second token.

Claim 49 (Previously Presented): The computer program product of claim 48 wherein each token of said one or more tokens is a physical token assigned to said user, a passphrase, or a biometric identifier.

Claim 50 (Previously Presented.): The computer program product of claim 49 wherein said biometric identifier is a finger print pattern or a retinal image.